

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1-6 (cancelled)

7. (previously presented) A method wherein a trusted party authenticates, for the benefit of a third party, that a customer using an account during an online transaction is the actual owner of said account, said method comprising:

requesting, by said trusted party from said customer, of an identity authenticating password;

verifying, by said trusted party, that said identity authenticating password from said customer matches a password previously designated for said account; and

notifying a third party, by said trusted party, that said customer is the actual owner of said account when said identity authenticating password entered by said customer matches the password that was previously designated for said account, whereby said notified third party desires verification as to the identity of said customer before proceeding with an online transaction with said customer.

8. (previously presented) A method as recited in claim 7 wherein said trusted party is an issuer financial institution and said third party is an online merchant, whereby said online merchant conducts a financial transaction with said customer, and wherein said account of said customer is maintained by said issuer financial institution.

9. (previously presented) A method as recited in claim 7 further comprising:

querying an access control server to determine if an account of said customer is enrolled in a payment authentication service.

10. (previously presented) A method as recited in claim 9 wherein the access control server determines if said customer account is enrolled by verifying that said customer account is contained in a database of enrolled customer accounts.

11. (previously presented) A method as recited in claim 9 further comprising:

querying a directory server to verify that said customer account is associated with an

issuer financial institution that is participating in said payment authentication service, whereby said customer account is not enrolled with said payment authentication service if said customer account is not associated with an issuer financial institution.

12. (previously presented) A method as recited in claim 11 further comprising:

sending to said third party's computer system an Internet address for said access control server, said Internet address passing through said directory server before reaching said third party's computer system, whereby said Internet address for said access control server allows said third party to directly communicate with said access control server.

13. (previously presented) A method as recited in claim 9 further comprising:

reviewing a memory device controlled by said third party to verify that said customer account is associated with an issuer financial institution participating in said payment authentication service, whereby said customer account is not enrolled with said payment authentication service if said customer account is not associated with an issuer financial institution.

14. (previously presented) A method as recited in claim 7 further comprising:

generating, by said trusted party, a digitally signed transaction receipt using a signature key of said trusted party; and

sending, by said trusted party, of a digitally signed transaction receipt to said third party, whereby the digitally signed transaction receipt confirms to said third party that the identity of said customer has been authenticated.

15. (previously presented) A method as recited in claim 14 wherein said transaction receipt includes a number associated with said customer account, a transaction payment amount, and a transaction payment date.

16. (previously presented) A method as recited in claim 7 further comprising:

sending, by said trusted party, of a card authentication verification value to said third party, the card authentication verification value containing a unique value for said customer account and a specific payment transaction, whereby said card authentication verification value uniquely identifies a specific authenticated payment transaction.

17. (previously presented) A method as recited in claim 8 further comprising:
verifying, by said third party, of said digitally signed transaction receipt such that said third party is assured that said transaction receipt was sent from a specific trusted party.
18. (previously presented) A method as recited in claim 7 further comprising:
sending, by said third party, of an authorization message to an issuer financial institution to verify said customer account has adequate credit for a requested purchase.
19. (previously presented) A method as recited in claim 7 wherein said customer enrolls in said payment authentication service, the method further comprising:
receiving, by said trusted party, of enrollment information entered at an enrollment Internet web site by said customer;
verifying, by said trusted party, that said enrollment information substantially matches information contained within a pre-existing database of customer information; and
storing said customer account information in a database for enrolled customer accounts.
20. (previously presented) A method performed by a payment authentication service wherein a trusted party authenticates, for the benefit of a third party, that a customer using an account during an online transaction is the actual owner of said account, said method comprising:
sending a payment request message to a customer software module from a third-party software module;
receiving a payment request message at an access control server that is operated by said trusted party, said payment request message being sent to said access control server from said customer software module;
requesting, by said trusted party, of a password from said customer;
verifying, by said trusted party, that said password entered by said customer is valid; and
sending, by said trusted party, a payment response message to a third-party software module, said payment response message containing an authentication status indicator.
21. (previously presented) A customer software module containing computer code used with a payment authentication service wherein an issuer financial institution authenticates, for the benefit of a third party, that a customer using an account during an online transaction is the actual owner of said account, said customer software module effecting the following:
receiving a payment request message from a third party that requests the initiation of a

payment authentication service wherein the identity of a customer will be authenticated;

sending said payment request message to an access control server operated by said issuer financial institution, said customer having an account with said issuer financial institution; and

receiving a request from said access control server for said customer to enter a password used to verify the identity of said customer.

22. (previously presented) A third-party computer used with a payment authentication service wherein an issuer financial institution authenticates, for the benefit of a third party, that a customer using an account during an online transaction is the actual owner of said account, said third-party computer comprising:

an Internet web page configured to present and receive information from said customer;

a plug-in software module configured to send a payment request message to a customer software module, said payment request message causing an access control server to query said customer for a password, said third-party plug-in software module configured to receive a payment response message which contains an authentication status, said authentication status serving to inform said third-party computer system whether or not the identity of said customer has been authenticated; and

a payment database for storing said authentication status, transaction data and payment data.

23. (previously presented) A method performed by an enrollment server used with a payment authentication service wherein an issuer financial institution authenticates, for the benefit of a third party, that a customer using an account during an online transaction is the actual owner of said account, said method comprising:

supporting an enrollment Internet web page to present and receive information from a customer for the purpose of enrolling said customer into said payment authentication service;

presenting questions to said customer intended to illicit answers from said customer useful for verifying the identity of said customer;

if the identity of said customer is verified, providing a customer software module to a customer client system, said customer software module containing computer code that will allow said customer to participate in said payment authentication service.

Claims 24-31 (cancelled)